Journal of Advances in Mathematics vol 16 (2019) ISSN: 2347-1921 https://rajpub.com/index.php/jam

DOI: https://doi.org/10.24297/jam.v16i0.8167

A way to compute a greatest common divisor in the Galois field $(\mathbf{GF}\ (2^n))$

W.Eltayeb Ahmed

Mathematics and Statistics Department, Faculty of Science, Al-Imam Mohammad Ibn Saud Islamic University, Saudi Arabia

waahmed@imamu.edu.sa

Abstract

This paper presents how the steps that used to determine a multiplicative inverse by method based on the Euclidean algorithm, can be used to find a greatest common divisor for polynomials in the Galois field $(\mathrm{GF}\ (2^n))$.

Keywords: Greatest common divisor, multiplicative inverse, irreducible polynomial, extended Euclidean algorithm, Bezout identity.

1 Introduction

The problem considered in this paper is computation of the greatest common divisor of nonzero polynomials $M(x)$ and $P(x)$, where $\deg M(x) < \deg P(x)$ in the Galois field $F(x) = \mathrm{GF}\ (2^n)$, $n \geq 2$, which appears in many situations in cryptography. The process of computing the greatest common divisor is inseparable from computing the multiplicative inverse. In general, the extended Euclidean algorithm can be used to compute them.

To compute a greatest common divisor, we will use the more elegant theorem (presented in the paper [1]), which computes the multiplicative inverse in simple and straightforward steps.

2 Basic Definitions

2.1 Greatest Common Divisor (gcd)

Let $M(x)$ and $P(x)$ in $F(x)$, then the greatest common divisor of $M(x)$ and $P(x)$, denoted $gcd(M(x), P(x))$ is the polynomial of greatest degree in $F(x)$ which divides both $M(x)$ and $P(x)$. [2]

2.2 Irreducible polynomial

A polynomial $P(x) \in F(x)$, is irreducible in $F(x)$ if $P(x)$ can not be expressed as a product $A(x)B(x)$ of two polynomials $A(x)$ and $B(x)$ in $F(x)$ both of lower degree than the degree of $P(x)$. [3]

2.3 Multiplicative inverse (MI)

The multiplicative inverse of $M(x)$ modulo $P(x)$ is $M^{-1}(x)$ such that

$$M(x)M^{-1}(x) = 1(\ mod\ P(x)) \qquad \rightarrow (1)$$

We will denote it by $T[M(x)]$. [2]

3 Relationship between gcd and MI

Bezout identity can be stated as follow:

If $d(x) = gcd(M(x), P(x))$ for given polynomials $M(x)$ and $P(x)$ in $F(x)$, then there are two polynomials $A(x)$ and $B(x)$, (are not unique), such that

$$d(x) = A(x)M(x) + B(x)P(x) \quad \rightarrow (2)$$

If $d(x) = 1$, and since

$$B(x)P(x) = 0 \ (mod\ P(x)) \quad \rightarrow (3)$$

we get

$$A(x)M(x) = 1 \ (mod\ P(x)) \quad \rightarrow (4)$$

Hence $A(x)$ is a multiplicative inverse of $M(x)$ modulo $P(x)$, this means a multiplicative inverse only exists when the gcd is 1,

4 Theorem and corollaries

4.1 Theorem (proved in the paper [1]).

Given $M_1(x)$ and $P(x)$, if there are $q_1(x)$ and $r_1(x)$ such that

$$M_1(x)q_1(x) + r_1(x) = Q_1(x) \quad \rightarrow (5)$$

where $Q_1(x) = P(x) + 1$, then

$$T[M_1(x)] = \begin{cases} q_1(x), & if\ r_1(x) = 0 \\ q_1(x) + T\left[\dfrac{M_1(x)}{r_1(x)}\right], & if\ r_1(x) \neq 0 \end{cases} \quad \rightarrow (6)$$

And suppose that $r_1(x) \neq 0$, and $M_2(x) = r_1(x) + 1$, if there are $q_i(x)$ and $r_i(x)$ such that

$$M_i(x)q_i(x) + r_i(x) = Q_i(x) \ , \ i \geq 2 \quad \rightarrow (7)$$

where $M_{i+1}(x) = r_i(x)$, and $Q_i = M_{i-1}$ then when $r_i(x) = 1$,

$$T[M_1(x)] = T_i[M_1(x)] = q_i(x)T_{i-1}[M_1(x)] + T_{i-2}[M_1(x)] \quad \rightarrow (8)$$

where $T_0[M_1(x)] = 1$, $T_1[M_1(x)] = q_1(x)$.

4.2 Corollary (1)

Let $d(x) = gcd(M_1(x), P(x))$, with $q_1(x)$ and $r_1(x)$ satisfing the hypotheses of the theorem, then

$$d(x) = \begin{cases} 1, & if\ r_1(x) = 0 \\ M_1(x), & if\ r_1(x) = 1 \end{cases} \quad \rightarrow (9)$$

Proof:

From Eq (6), when $r_1(x) = 0$, there is a multiplicative inverse, $T[M_1(x)] = q_1(x)$. So $d(x) = 1$.

When $r_1(x) = 1$, Eq (5) becomes

$$M_1(x)q_1(x) = P(x) \quad \rightarrow (10)$$

Implying that $M_1(x) | P(x)$, giving $d(x) = M_1(x)$.

We note that when $r_1(x) = 1$, $P(x)$ must be a reducible polynomial.

4.3 Corollary (2)

Let $d(x) = gcd(M_1(x), P(x))$, and $q_i(x)$ and $r_i(x)$ satisfing the hypotheses of the theorem, then

$$d(x) = \begin{cases} r_{i-1}, & if \quad r_i(x) = 0 \\ 1, & if \quad r_i(x) = 1 \end{cases} \quad \rightarrow (11)$$

Proof**:**

$d(x) = gcd(M_1(x), P(x))$

$= gcd(M_1(x), Q_1(x) + 1)$

$= gcd(M_1(x), r_1(x))$

$= gcd\big(M_2(x) + 1, Q_2(x)\big)$

$= gcd\big(M_2(x) + 1, r_2(x)\big)$

When $r_2(x) = 0$

$d(x) = gcd(M_2(x) + 1,0)$

$= M_2(x) + 1$

$= r_1(x)$

If $r_2(x) \neq 0$

$d(x) = gcd\big(M_2(x) + 1, r_2(x)\big)$

$= gcd\big(M_3(x), Q_3(x)\big)$

$= gcd\big(M_3(x), r_3(x)\big)$

$= gcd\big(M_4(x), Q_4(x)\big)$

$= \cdots$

$= gcd\big(M_{i+1}(x), Q_{i+1}(x)\big)$

$= gcd\big(r_i(x), M_i(x)\big)$

$= gcd\big(r_i(x), r_{i-1}(x)\big)$

When $r_i(x) = 0$, $i > 2$

$d(x) = gcd\big(0, r_{i-1}(x)\big)$

$= r_{i-1}(x)$

When $r_i(x) = 1$, there is $T[M_1(x)]$, so $gcd(M_1(x), P(x)) = 1$.

We note that when $r_i(x) = 0$, $P(x)$ must be a reducible polynomial.

5 Procedure to find gcd

To find $gcd(M_1(x), P(x))$, we seek for polynomials $q_1(x)$ and $r_1(x)$ satisfying Eq (5), then from Eq (9), we can find $gcd(M_1(x), P(x))$.

If $r_1(x)$ is neither 0 nor 1, then we put $M_2(x) = r_1(x) + 1$, and seek for polynomials $q_i(x)$ and $r_i(x)$ satisfying Eq (7), and by using Eq (11), we can find $gcd(M_1(x), P(x))$.

6 Examples

6.1 In Advanced Encryption Standard (AES), $F(x) = \mathrm{GF}(2^8)$, and the irreducible polynomial is $P(x) = x^8 + x^4 + x^3 + x + 1$. If $A(x) = x^6 + x^5 + x^4 + x^3 + x + 1$, $B(x) = x^6 + x^5 + x^4 + x^3 + x$.

i	$A(x)$	$q(x)$	$r(x)$	$Q(x)$
1	$x^6 + x^5 + x^4 + x^3 + x + 1$	$x^2 + x$	0	$x^8 + x^4 + x^3 + x$

From Eq (6), $T[A(x)] = x^2 + x$.

From Eq (9), $gcd(A(x), P(x)) = 1$.

i	$B(x)$	$q(x)$	$r(x)$	$Q(x)$
1	$x^6 + x^5 + x^4 + x^3 + x$	$x^2 + x$	$x^2 + x$	$x^8 + x^4 + x^3 + x$
2	$x^2 + x + 1$	$x^4 + x + 1$	$x + 1$	$x^6 + x^5 + x^4 + x^3 + x$
3	$x + 1$	x	1	$x^2 + x + 1$

$r_3(x) = 1$, from Eq (8),

$$T[B(x)] = \mathrm{q}_3(x)T_3[B(x)] + T_2[B(x)]$$

$$= x[(x^4 + x + 1)(x^2 + x) + 1] + x^2 + x$$

$$= x^7 + x^6 + x^4 .$$

From Eq (11), $gcd(B(x), P(x)) = 1$.

6.2 For $F(x) = \mathrm{GF}(2^n)$, Take $P(x) = x^6 + x^5 + x^4 + x^3 + x^2 + 1$. If $A(x) = x^4 + x^3 + 1$, $B(x) = x^4 + x^3$.

i	$A(x)$	$q(x)$	$r(x)$	$Q(x)$
1	$x^4 + x^3 + 1$	$x^2 + 1$	1	$x^6 + x^5 + x^4 + x^3 + x^2$

From Eq (9), $gcd(\mathrm{A}(x), P(x)) = A(x) = x^4 + x^3 + 1$.

i	$B(x)$	$q(x)$	$r(x)$	$Q(x)$

1	x^4+x^3	x^2+1	x^2	$x^6+x^5+x^4+x^3+x^2$
2	x^2+1	x^2+x+1	$x+1$	x^4+x^3
3	$x+1$	$x+1$	0	x^2+1

From Eq (11),

$$gcd\big(B(x),P(x)\big)=r_2(x)$$

$$=x+1.$$

Conclusions

This paper demonstrates how simply and efficiently we can compute the gcd of $M(x)$ and $P(x)$ using the method presented in [1].

References

1. W. Eltayeb Ahmed, Some Techniques to Compute Multiplicative Inverses for Advanced Encryption Standard, Journal of Advances in Mathematics, Vol 16 (2019) ISSN: 2347-1921. https://cirworld.com/index.php/jam
2. A. Menezes, P. van Oorschot, and S. Vanstone, Handbook of Applied Cryptography, CRC Press, New York, 1997.
3. John B. Fealenigh , A First Course in Abstract Algebra, 7 th edition, Pearson press , 2002.